
Claims

What is claimed is:

1. A method for providing a cryptographic ticket to a trusted module allowing that module to issue a pre-determined number of public-key certificates.
2. A computer system based on the method of 1.
3. A computer system based on the method of claim 1 where the trusted module is a hardware token such as a USB token or a smartcard.
4. A method based on claim 1 where the cryptographic ticket is a public-key or private-key certificate.
5. A computer system based on the method of 4.
6. A computer system based on the method of claim 4 where the trusted module is a hardware token such as a USB token or a smartcard.
7. A method based on claim 1 where the pre-determined number of certificates that can be issued is determined by information within the provided cryptographic ticket.
8. A computer system based on the method of 7.

A computer system based on the method of claim 7 where the trusted module is a hardware token such as a USB token or a smartcard.